CLAIMS

We claim:

1. A method for creating a unique authoritative electronic record, comprising the steps of:

receiving an electronic record into a repository, wherein the repository is contained on an electronic device that stores and executes software;

generating a receipt, wherein the receipt includes information relating to the electronic record;

generating identifying information that includes a provable representation of the receipt;

prepending the receipt to a beginning of the record;

appending the identifying information to an ending of the record; and,

storing the record with the prepended receipt and the appended identifying information as the unique authoritative record in the repository.

2. The method of claim 1, wherein the step of receiving a record further comprises the step of attaching a time-stamp to the electronic record, wherein the time-stamp includes a time and a date when the electronic record was received in the repository and identification information.

3. The method of claim 1, wherein the receipt comprises a digital signature made with a private key of the repository.

4. The method of claim 1, wherein the repository creates a copy of the authoritative record by copying the record and all information appended to the ending of the record.

5. A method for obtaining a digital signature on an authoritative record stored in a secure environment, comprising the steps of:

receiving a request to sign the authoritative record;

computing a partial message digest of a proper subset of the authoritative record;

computing a complement of the proper subset;

sending the partial message digest and at least the complement of the proper subset of the authoritative record to a remote location;

computing a message digest, at the remote location, using the partial message digest and the complement of the subset; and,

creating a digital signature with the use of the message digest and a private key.

6. The method of claim 5, wherein the proper subset of the authoritative record comprises information at a beginning of the authoritative record.

7. The method of claim 5, wherein the complement of the proper subset of the authoritative record comprises an electronic record and ending information that is appended an end of the record.

8. The method of claim 5, wherein the step of sending further comprises the steps of

sending the partial message digest and

the complement of the proper subset of the authoritative record to the remote location.

9. The method of claim 5, wherein software associated with the secure environment is used at the remote location.

10. The method of claim 5, further comprising the step of:

transmitting the digital signature to the secure environment.

11. A method for creating a unique authoritative record, obtaining and validating a digital signature on the authoritative record, and upon successful validation creating a unique revised authoritative record, comprising the steps of:

receiving a record in a secure environment, wherein the secure environment is connected to a network and comprises at least one server that stores and executes software;

generating a receipt, wherein the receipt includes information relating to the record;

generating identifying information that includes a provable representation of the receipt;

prepending the receipt to a beginning of the record;

appending the identifying information to an ending of the record;

storing the record with prepended receipt and appended information as the unique authoritative record;

receiving a request to sign the authoritative record;

computing a partial message digest of a proper subset of the authoritative record;

sending the partial message digest and at least a complement of the proper subset of the authoritative record to a remote location;

computing a message digest, at the remote location, using the partial message digest and the complement of the subset;

creating a digital signature with the use of the message digest and a private key;

transmitting the digital signature to the secure environment;

validating the digital signature in the secure environment, and upon affirmative validation;

revising the authoritative record with the digital signature to create a revised authoritative record.

12. The method of claim 11, wherein the step of receiving a record further

comprises time-stamping the record, wherein a time-stamp comprising a time and date the record was received and identification information is attached to the record and the time-stamped record is used as the record in subsequent steps.

13. The method of claim 11, wherein the receipt is a digital signature that is made with a private key of the secure environment.

14. The method of claim 11, wherein the proper subset of the authoritative record comprises information at a beginning of the authoritative record.

15. The method of claim 11, wherein the complement of the proper subset of the authoritative record comprises the record and ending information that is appended an end of the record.

16. The method of claim 11, wherein the step of sending further comprises the steps of sending the partial message digest and the complement of the proper subset of the authoritative record to the remote location in two separate transmissions.

17. The method of claim 11, wherein software associated with the secure environment is used at the remote location.

18. A method for creating and validating at least one digital signature for an electronic authoritative record maintained in a secure environment, wherein control is maintained in the secure environment by software and at least one server, and a copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic authoritative record's integrity, the method comprising the steps of:

receiving an electronic record in the secure environment;

generating at least some first information comprising a receipt of the electronic record by the secure environment;

defining a beginning information as all information prepended to a beginning of the record and comprising the first information;

generating at least some second information comprising a provable representation of the first information, wherein the provable representation of the first information is mathematically related to the first information;

defining an ending information as all information appended to an end of the record and comprising the second information;

creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning of the electronic record and the ending information is appended to the end of the electronic record;

storing the authoritative record in the secure environment;

making a perceivable copy of the authoritative record by copying only the electronic record and the ending information;

transmitting the perceivable copy of the authoritative record to a remote location;

receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record by:

generating a partial message digest of the beginning information at the secure environment;

transmitting the partial message digest from the secure environment to the remote location,

completing a message digest of the authoritative record at the remote location with the use of the partial message digest and the perceivable copy; and,

creating a digital signature using the message digest at the remote location and a private key to produce a digital signature of the authoritative record;

transmitting the digital signature from the remote location to the secure environment;

receiving the digital signature in the secure environment;

validating the digital signature in the secure environment with the use of the digital signature, a corresponding public key of the private key, and a separately computed message digest of the authoritative record in the secure environment, and upon affirmative validation of the digital signature;

generating a revised authoritative record by prepending digital signature information comprising the digital signature to a beginning of the authoritative record, wherein the digital signature information is thereby included in the beginning information, appending signature information comprising of a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information; and,

storing the revised authoritative record in the secure environment.

19. The method of claim 18, wherein the step of generating a revised authoritative record, further comprises:

prepending a signature receipt to the beginning information so that the signature receipt becomes part of the beginning information, wherein the signature receipt comprises a unique representation of the revised authoritative record; and,

appending identifying information to the ending information so that the identifying information becomes part of the ending information, wherein the identifying information comprises a provable representation of the signature receipt.

20. The method of claim 18, wherein software associated with the secure environment is stored and used at the remote location.

21. The method of claim 18, wherein the perceivable copy and the partial message digest are transmitted to the remote location in a same transmission.

22. The method of claim 18, further comprising the steps of:

sending copies of the revised authoritative record to one or more remote locations by treating the revised authoritative record as the authoritative record and repeating the steps of:

making a perceivable copy;

transmitting the perceivable copy;

receiving the perceivable copy;

generating a partial message digest;

transmitting the partial message digest;

completing a message digest,

creating a digital signature;

transmitting the digital signature;

validating the digital signature; and,

generating a revised authoritative record.

23. The method of claim 19, further comprising the steps of:

sending copies of the revised authoritative record to one or more remote locations by treating the revised authoritative record as the authoritative record and repeating the steps of:

making a perceivable copy;

transmitting the perceivable copy;

receiving the perceivable copy;

generating a partial message digest;

transmitting the partial message digest;

completing a message digest,

creating a digital signature;

transmitting the digital signature;

validating the digital signature;

generating a revised authoritative record;

prepending a signature receipt; and,

appending identifying information.

24. The method of claim 18, wherein the step of receiving an electronic record further comprises: time-stamping the electronic record with a time-stamp that includes a time and date of receipt, and identification information and the time-stamped record is used as the electronic record in the subsequent steps.

25. The method of claim 18, wherein the first information comprises a digital signature made with a private key of the secure environment.

26. The method of claim 18, wherein the provable representation of the first information comprises a message digest that was used to generate the first information.

27. The method of claim 18, wherein the step of transmitting the perceivable copy, further comprises:

transmitting a cryptographic version of the copy.

28. The method of claim 18, wherein the partial message digest includes information necessary to continue the creation of the message digest at the remote location.

29. The method of claim 18, wherein the step of validating further comprises the steps of:

decrypting the digital signature with a public key; and,

comparing the decrypted digital signature with a representation of the authoritative record stored in the secure environment.

30. A computer readable medium for storing a program that allows a user to receive, and digitally sign a copy of an electronic record that is stored in a remote location, wherein the program provides for the user to:

receive a proper subset of the electronic record, wherein the proper subset of the electronic record allows the user to view, store and print the record, and when the user is ready, to;

sign the electronic record, wherein the program requests and receives at least a complement of the proper subset of the electronic record, and the user then uses the proper subset, the complement of the subset, and a private key to digitally sign the record.

31. The computer readable medium of claim 30, wherein the program provides for transmission of the digital signature to the remote location.

32. A method for digitally signing an electronic record received from a secure environment, wherein the electronic record consists of a first portion and a second portion, the method comprising the steps of:

receiving the first portion of the electronic record from the secure environment, wherein the first portion allows a user to view, print or store the electronic record;

receiving a partial message digest of the electronic record from the secure environment wherein the partial message digest is related to the second portion of the electronic record;

generating a message digest of the electronic record using the first portion and the partial message digest; and,

creating a digital signature of the electronic record using the message digest and a private key.

33. The method of claim 32, further comprising the step of:

transmitting the digital signature to the secure environment.

34. An apparatus for creating and storing a unique authoritative record, comprising:

at least one server, connected to a network, that stores and executes software for receiving a record in a secure environment wherein the secure environment is created by the server and the software; wherein the software provides for:

generating a receipt, wherein the receipt includes information relating to the record;

generating identifying information that includes a provable representation of the receipt;

prepending the receipt to a beginning of the record;

appending the identifying information to an ending of the record; and,

storing the record with prepended receipt and appended information as the unique authoritative record in the secure environment.

35. The apparatus of claim 34, wherein the record is time-stamped, with a time and date the record was received and with identification information, immediately after the record is received in the secure environment.

36. The apparatus of claim 34, wherein the receipt comprises a digital signature made with a private key of the secure environment.

37. The apparatus of claim 34, wherein the secure environment creates a copy of the authoritative record by copying the record and all information appended to the ending of the record.

38. An system for obtaining a digital signature on an authoritative record that is stored in a secure environment, comprising:

a server that stores and executes software that creates the secure environment and at least one computer at a remote location that stores and executes at least of portion of the software, wherein the software provides for:

receiving a request from the remote location to sign the authoritative record;

computing a partial message digest at the secure environment of a proper subset of the authoritative record;

sending the partial message digest and at least a complement of the proper subset of the authoritative record to the remote location;

computing a message digest, at the remote location, using the partial message digest and the complement of the subset; and,

creating a digital signature with the use of the message digest and a private key.

39. The system of claim 38, wherein the proper subset of the authoritative record comprises information at a beginning of the authoritative record.

40. The system of claim 38, wherein the complement of the proper subset of the authoritative record comprises a record and ending information that is appended an end of the record.

41. The system of claim 38, wherein the partial message digest and the complement of the proper subset of the authoritative record are sent to the remote location in two separate transmissions.

42. The system of claim 38, wherein the digital signature is transmitted to the secure environment.

43. A system for creating a unique authoritative record, obtaining and validating a digital signature on the authoritative record, and upon successful validation creating a unique revised authoritative record, comprising:

at least one server, connected to a network, that stores and executes software that creates a secure environment and at least one computer at a

remote location that stores and executes at least of portion of the software, wherein the software provides for:

receiving a record in the secure environment;

generating a receipt, wherein the receipt includes information relating to the record;

generating identifying information that includes a provable representation of the receipt;

prepending the receipt to a beginning of the record;

appending the identifying information to an ending of the record;

storing, in the secure environment, the record with prepended receipt and appended information as the unique authoritative record;

receiving a request, from the remote location, to sign the authoritative record;

computing a partial message digest of a proper subset of the authoritative record at the secure environment;

sending the partial message digest and at least a complement of the proper subset of the authoritative record to the remote location;

computing a message digest, at the remote location, using the partial message digest and the complement of the subset;

creating a digital signature with the use of the message digest and a private key;

transmitting the digital signature from the remote location to the secure environment;

validating the digital signature in the secure environment, and upon affirmative validation;

revising the authoritative record with the digital signature to create a revised authoritative record.

44. The system of claim 43, wherein the record is time-stamped, immediately after it is received by the secure environment, with a time-stamp comprising a time and date the record was received and identification information.

45. The system of claim 43, wherein the receipt is a digital signature that is made with a private key of the secure environment.

46. The system of claim 43, wherein the proper subset of the authoritative record comprises information at a beginning of the authoritative record.

47. The system of claim 43, wherein the complement of the proper subset of the authoritative record comprises the record and ending information that is appended an end of the record.

48. The system of claim 43, wherein the partial message digest and the complement of the proper subset of the authoritative record are sent to the remote location in two separate transmissions.

49. A system for creating and validating at least one digital signature on an electronic authoritative record that is maintained in a secure environment, wherein a copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic authoritative record's integrity, the system comprising:

at least one server, connected to a network, that stores and executes software that creates the secure environment and at least one computer at a remote location that stores and executes a portion of the software, wherein the software provides for:

receiving an electronic record in the secure environment;

generating at least some first information comprising a receipt of the electronic record by the secure environment;

defining a beginning information as all information prepended to a beginning of the record and comprising the first information;

generating at least some second information comprising a provable representation of the first information, wherein the provable representation of the first information is mathematically related to the first information;

defining an ending information as all information appended to an end of the record and comprising the second information;

creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning of the electronic record and the ending information is appended to the end of the electronic record;

storing the authoritative record in the secure environment;

making a perceivable copy of the authoritative record by copying only the electronic record and the ending information;

transmitting the perceivable copy of the authoritative record to a person at the remote location;

receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record by:

generating a partial message digest of the beginning information at the secure environment;

transmitting the partial message digest from the secure environment to the remote location,

completing a message digest of the authoritative record at the remote location with the use of the partial message digest and the perceivable copy; and,

creating a digital signature using the message digest at the remote location and a private key to produce the digital signature of the authoritative record;

transmitting the digital signature from the remote location to the secure environment;

validating the digital signature in the secure environment with the use of the digital signature, a corresponding public key of the private key, and a

separately computed message digest of the authoritative record in the secure environment, and upon affirmative validation of the digital signature;

generating a revised authoritative record by prepending digital signature information comprising the digital signature to a beginning of the authoritative record, wherein the digital signature information is thereby included in the beginning information, appending signature information comprising of a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information; and,

storing the revised authoritative record in the secure environment.

50. The system of claim 49, wherein generating a revised authoritative record, further comprises:

prepending a signature receipt to the beginning information so that the signature receipt becomes part of the beginning information, wherein the signature receipt comprises a unique representation of the revised authoritative record; and,

appending identifying information to the ending information so that the identifying information becomes part of the ending information, wherein the identifying information comprises of a provable representation of the signature receipt.

51. The system of claim 49, wherein the perceivable copy and the partial message digest are transmitted to the remote location in a same transmission.

52. The system of claim 49, wherein the software further provides for sending copies of the revised authoritative record to one or more remote locations by treating the revised authoritative record as the authoritative record and repeating the steps of:

making a perceivable copy;

transmitting the perceivable copy;

receiving the perceivable copy;
generating a partial message digest;
transmitting the partial message digest;
completing a message digest,
creating a digital signature;
transmitting the digital signature;
validating the digital signature; and,
generating a revised authoritative record.

53. The system of claim 50, wherein the software further provides for sending copies of the revised authoritative record to one or more remote locations by treating the revised authoritative record as the authoritative record and repeating the steps of:

making a perceivable copy;
transmitting the perceivable copy;
receiving the perceivable copy;
generating a partial message digest;
transmitting the partial message digest;
completing a message digest,
creating a digital signature;
transmitting the digital signature;
validating the digital signature;
generating a revised authoritative record;
prepending a signature receipt; and,
appending identifying information.

54. The system of claim 49, wherein the electronic record is time-stamped immediately after being received in the secure environment, and the time-stamp comprises a time and date of receipt, and identification information.

55. The system of claim 49, wherein the first information comprises a digital

signature made with a private key of the secure environment.

56. The system of claim 49, wherein the provable representation of the first information comprises a message digest that was used to generate the first information.

57. The system of claim 49, wherein a cryptographic version of the perceivable copy is transmitted to the remote location.

58. The system of claim 49, wherein the partial message digest includes information necessary to continue the creation of the message digest at the remote location.

59. The system of claim 49, wherein validation further comprises:

decrypting the digital signature with a public key; and,

comparing the decrypted digital signature with a representation of the authoritative record stored in the secure environment.

60. An apparatus for digitally signing an electronic record that is received from a secure environment, wherein the electronic record consists of a first portion and a second portion, comprising:

a computer that stores and executes software, wherein the software provides for:

receiving the first portion of the electronic record from the secure environment, wherein the first portion allows a user to view, print or store the electronic record;

receiving a partial message digest of the second portion of the electronic record from the secure environment;

generating a message digest of the electronic record using the first portion and the partial message digest; and,

creating a digital signature of the electronic record using the message digest and a private key.

61. The apparatus of claim 60, wherein the computer transmits the digital signature to the secure environment.